APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/504,005	02/14/2000	Sami Boutros	CISCO-1935	7397

7590   06/03/2005

JONATHAN VELASCO
SIERRA PATENT GROUP, LTD
P.O. BOX 6149
STATELINE, NV 89449

EXAMINER
KLIMACH, PAULA W

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 06/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/504,005	BOUTROS ET AL.
	Examiner	Art Unit
	Paula W. Klimach	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 February 2005*.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

U.S. Patent and Trademark Office

PTOL-326 (Rev. 1-04)   Office Action Summary   Part of Paper No./Mail Date 20050524

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 02/10/2005. Original application contained Claims 1-26. The amendment filed on 02/10/05 have been entered and made of record. Therefore, presently pending claims are 1-26.

Response to Arguments

Applicant's arguments filed 02/10/05 have been fully considered but they are not persuasive because of following reasons.

Applicant argued that there is not teaching whatsoever of transmitting the packet to an inspection module in Dutta. This is not found persuasive. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., <u>transmitting</u> the packet to an inspection module) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., separate modules for <u>providing different tests</u>) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

The applicant argues further that there is not mention of new modules that may be loaded during execution of the firewall process. The module that is loaded during the execution of the firewall process is the pertinent rule that is fetched and processed in the section that is quoted by the applicant (column 5 lines 1-12).

The applicant argues further that there is no mention anywhere in the O'Brien document of modules that monitor packets being sent between systems. This is not persuasive. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., modules that monitor packets being sent between systems) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the knowledge is generally available to one of ordinary skill in the art.

In reference to claim 6, in response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., s firewall core that monitors a memory for inspection modules that are loaded into a memory during operation of the firewall system) are not recited in the rejected claim(s).

Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the knowledge is generally available to one of ordinary skill in the art.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., module that is loaded into a memory monitored by the firewall core during operation of the firewall system) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5

USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones,* 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992).

In this case, the knowledge is generally available to one of ordinary skill in the art.

The examiner asserts that Dutta and O'Brien does teach or suggest the subject matter

broadly recited in independent Claims 1, 6, 10, 15, 21. Dependent Claims 2-5, 7-9, 11, 13-14,

16-17, 19-20, 22-23, and 25-26 are also rejected at least by virtue of their dependency on

independent claims and by other reason set forth in this office action. Accordingly, rejections for

claims 1-11, 13-17, 19-23, and 25-26 are respectfully maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1.   **Claims 1-26** are rejected under 35 U.S.C. 103(a) as being unpatentable over Dutta (U.S.

Patent 6,574,666 B1) in view of O'Brien et al. (6,658,571 B1).

In reference to claim 1, Dutta suggests a firewall device having a plurality of

communication interfaces, a firewall system comprising: a) a firewall core connected to each

said communication interface (column 4 lines 63-66); said firewall core configured to receive

data packets from said interfaces for inspection (column 2 lines 60-65).

The firewall core utilizes a library of rules that can be downloaded from a database

(column 3 lines 15-25); therefore Dutta discloses receiving security information from a separate

subsystem, the database. Dutta does not disclose the separate subsystem consisting of at least

one inspection module coupled for communication to said firewall core, said inspection module

configured to provide protocol inspection of data packets, said inspection module is further

configured to be installed during the operation of the firewall system.

However, O'Brien disclose the separate subsystem consisting of at least one inspection

module coupled for communication to the user space, said inspection module configured to

provide protocol inspection of data (column 3 lines 39-56), said inspection module is further

configured to be installed during the operation of the system (column 3 lines 56-64).

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to use security modules as in O'Brien to provide protocol inspection in the system

of Dutta. One of ordinary skill in the art would have been motivated to do this because security

information that is application and resource specific which would reduce the damage that

malicious software can cause in the event that malicious software is accidentally executed

without additional hardware, or modification to the individual software applications or the

underlying operating system.

In reference to claim 6, Dutta suggests a firewall device having a plurality of

communication interfaces, a firewall core configured to be coupled to at least one inspection

module, said firewall core comprising: a communication unit operatively coupled to the

communication interfaces (column 4 lines 63-66).

The firewall core in the system of Dutta utilizes a library of rules that can be downloaded

from a database (column 3 lines 15-25); therefore Dutta discloses receiving security information

from a separate subsystem, the database. However Dutta does not disclose a set of callback

functions, retrieved from said inspection module, each said function providing communication

between said firewall core and said inspection module. In addition the firewall core disclosed by Dutta is not configured to monitor a memory to determine when a new inspection module is loaded into said memory (column 5 lines 15-27).

O'Brien discloses a set of callback functions, retrieved from said inspection module, each said function providing communication between the security master and said inspection module (column 5 lines 15-27). In addition the system of O'Brien is configured to monitor a memory to determine when a new inspection module is loaded into said memory (column 5 lines 28-46).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use callback functions from security modules as in O'Brien to provide protocol inspection in the system of Dutta. One of ordinary skill in the art would have been motivated to do this because callback functions allow the security modules to communicate with the user space so that security information that is application and resource specific which would reduce the damage that malicious software can cause in the event that malicious software is accidentally executed without additional hardware, or modification to the individual software applications or the underlying operating system.

In reference to claim 10, Dutta suggests a firewall device having a plurality of communication interfaces and a firewall core coupled to the communication interfaces, an inspection module to configured to couple with the firewall core, said inspection module comprising: a) an inspection unit configured to inspect and authorize data packets (column 5 lines 1-12).

The firewall core in the system of Dutta utilizes a library of rules that can be downloaded from a database (column 3 lines 15-25); therefore Dutta discloses receiving security information

from a separate subsystem, the database. However Dutta does not disclose a set of callback functions, retrieved from said inspection module, each said function providing communication between said firewall core and said inspection module. In addition the system disclosed by O'Brien is configured to monitor a memory to determine when a new inspection module is loaded into said memory (column 5 lines 15-27).

O'Brien discloses a set of callback functions, retrieved from said inspection module, each said function providing communication between the security master and said inspection module (column 5 lines 15-27). In addition the firewall core disclosed by Dutta is not configured to monitor a memory to determine when a new inspection module is loaded into said memory (column 5 lines 28-46).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use callback functions from security modules as in O'Brien to provide protocol inspection in the system of Dutta. One of ordinary skill in the art would have been motivated to do this because callback functions allow the security modules to communicate with the user space so that security information that is application and resource specific which would reduce the damage that malicious software can cause in the event that malicious software is accidentally executed without additional hardware, or modification to the individual software applications or the underlying operating system.

In reference to claims 15 and 21, Dutta suggests a firewall device having a firewall system including a firewall core, a method for adding protocol knowledge to the firewall system during runtime (column 3 lines 14-25).

However Dutta does not disclose a) loading an inspection module comprising new protocol inspection knowledge and a function table having a set of callback functions; to b) notifying the firewall core of said inspection module (column 3 lines 26-33); and c) communicating said set of callback functions to said firewall core.

O'Brien discloses a) loading an inspection module comprising new protocol inspection knowledge and a function table having a set of callback functions (column 5 lines 1-27); to b) notifying the security master of said inspection module (column 5 lines 12-27); and c) communicating said set of callback functions to the security master (column 5 lines 27-45).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use callback functions from security modules as in O'Brien to provide protocol inspection in the system of Dutta. One of ordinary skill in the art would have been motivated to do this because callback functions allow the security modules to communicate with the user space so that security information that is application and resource specific which would reduce the damage that malicious software can cause in the event that malicious software is accidentally executed without additional hardware, or modification to the individual software applications or the underlying operating system.

In reference to claim 2, wherein said inspection module is installed into a memory space monitored by said firewall core (Dutta column 4 lines 41-62).

In reference to claim 3, wherein said inspection module further comprises callback functions, said functions communicated to said firewall core and providing communication between said firewall core and said inspection module.

Dutta does not expressly disclose the use of callback functions which communicate to the

firewall core and providing communication between the firewall core and said inspection

module.

O'Brien discloses a set of callback functions, retrieved from said inspection module, each

said function providing communication between the security master and said inspection module

(column 5 lines 15-27)

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to use callback functions from security modules as in O'Brien to provide protocol

inspection in the system of Dutta. One of ordinary skill in the art would have been motivated to

do this because callback functions allow the security modules to communicate with the user

space so that security information that is application and resource specific which would reduce

the damage that malicious software can cause in the event that malicious software is accidentally

executed without additional hardware, or modification to the individual software applications or

the underlying operating system.

In reference to claim 4, wherein said inspection module is further configured to indicate

to said firewall core for which data packets said inspection module is configured to provide

inspection (Dutta column 4 line 66 to column 5 line 12).

In reference to claim 5, wherein said data packets intercepted by said firewall core further

includes session information comprising address and port data, said firewall core further

configured to map said session information to corresponding inspection modules (Dutta column

2 line 60 to column 3 line 5 in combination with column 4 lines 32-50). Packet Filter Router

rules are based on address and port information, therefore, the address and port information
obviously must be contained within the packets.

In reference to claim 7, wherein said communication unit is further configured to
intercept network data communicated via said network interfaces (Dutta column 3 lines 46-65).

In reference to claim 8, further comprising a session mapping unit, said data packets
intercepted by said firewall core further including session information comprising address and
port data, said firewall core further configured to map said session information to corresponding
inspection modules into a session mapping and store said session mapping into said session
mapping unit (Dutta column 2 line 60 to column 3 line 5 in combination with column 4 lines 32-
50). Packet Filter Router rules are based on address and port information, therefore, the address
and port information obviously must be contained within the packets.

In reference to claim 9, wherein said communication unit is further configured to
communicate packets between said communication interfaces and said inspection module for
inspection (Dutta column 4 line 63 to column 5 line 12).

In reference to claim 11, wherein said inspection unit is further configured to be installed
during the operation of the firewall core. The rules retrieved by the filter processor to update the
filter processor are retrieved during the operation of the filter processor.

In reference to claim 13, the firewall system of claim 1, wherein said inspection module
is further configured to indicate to said firewall core for which data packets said inspection
module is configured to provide inspection (Dutta column 5 lines 1-12).

In reference to claim 14, where in said inspection unit is further configured to receive and
inspect packets communicated from the firewall core (Dutta column 5 lines 5-12).

In reference to claim 16 and 22, further comprising enabling said inspection module, prior to communicating·said set of callback function to said firewall core. The new information is used to filter packets therefore the new rules, provided by the filter processor, are in an enabled state similar to the state of the inspection module.

In reference to claim 17 and 23, further comprising inspecting of packets by said inspection module, said packets communicated from the firewall core to said inspection module (Dutta column 5 lines 1-12).

In reference to claim 19 and 25, wherein said notifying the firewall core comprises transmitting a signal to the firewall core to indicate the installation of said inspection module (Dutta column 3 lines 25-32).

In reference to claim 20 and 26, further comprising indicating by said inspection module for which data packets said inspection module provides inspection (Dutta column 5 lines 1-12).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing
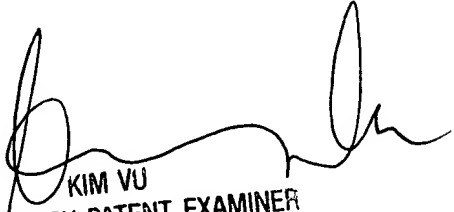
date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854.

The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Tuesday, May 31, 2005

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100